S04P10879M000

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－85493
（Ｐ２００３－８５４９３Ａ）
(43)公開日　平成15年３月20日(2003.3.20)

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
G06K 17/00		G06K 17/00	L	2C005
B42D 15/10	521	B42D 15/10	521	5B017
G06F 12/00	537	G06F 12/00	537 D	5B058
12/14	310	12/14	310 K	5B075
	320		320 A	5B082

審査請求　未請求　請求項の数３　ＯＬ　（全13頁）　最終頁に続く

(21)出願番号　特願2001－273543(Ｐ2001－273543)

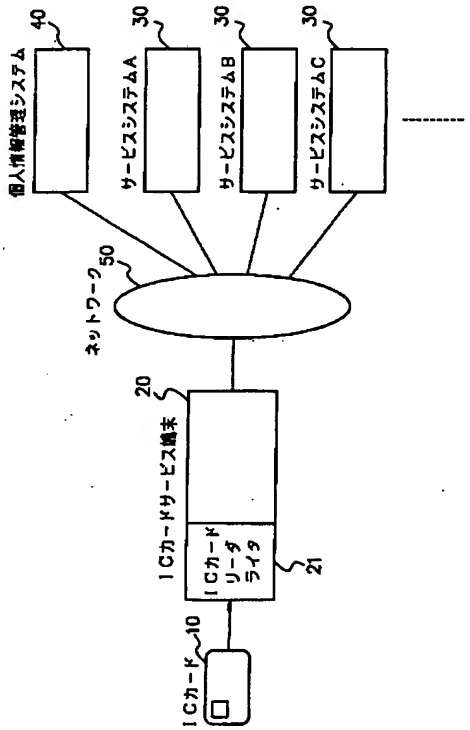
(22)出願日　平成13年９月10日(2001.9.10)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　林　良一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　▲高▼倉　健
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100069981
弁理士　吉田　精孝

最終頁に続く

(54)【発明の名称】個人情報統合管理システム及びそのプログラム並びにそのプログラムを記録した媒体

(57)【要約】
【課題】　複数のサービスシステムの情報連携によってユーザの意図しない個人情報が作り出されることがない個人情報統合管理システムを提供すること。
【解決手段】　ＩＣカード１０にサービスシステム３０毎の顧客認証に用いる鍵ペアを用意しておき、サービスシステム３０に公開鍵を送信する。サービスシステム３０ではユーザ用に作成した顧客ＩＤと受信した公開鍵に対しサービスシステム固有の暗号鍵により署名を行った電子証明書を作成し、ＩＣカード１０に送信する。サービスシステム３０から個人情報管理システム４０に情報連携処理要求があると、個人情報管理システム４０はサービスシステムＩＤと顧客ＩＤとからデータベースを検索し、ユーザＩＤを特定し、該ユーザＩＤの個人情報と関連付ける。ユーザが匿名でサービスを受けるための識別情報をサービスシステム毎に個別に用意することで、プライバシーを侵害するような情報連携を避ける。



1

【特許請求の範囲】

【請求項１】　少なくともユーザの個人情報を格納したＩＣカードと、ＩＣカードとの間でデータを送受信するためのＩＣカードリーダライタを有するＩＣカードサービス端末と、ＩＣカードにＩＣカード用アプリケーションプログラムを提供するとともにＩＣカードサービス端末に端末用アプリケーションプログラムを提供し、各アプリケーションプログラムが起動したＩＣカード及びＩＣカードサービス端末を通じてユーザにサービスを提供する複数のＩＣカードサービスシステムであってそのうちの少なくとも１つはＩＣカードに格納されたユーザの個人情報を利用してユーザにサービスを提供する複数のＩＣカードサービスシステムと、ＩＣカードに格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システムと、ＩＣカードサービス端末と複数のＩＣカードサービスシステムと個人情報管理システムとを接続するネットワークとからなり、前記個人情報管理システムは、前記サービスシステムの要求に基づき、該サービスシステムの顧客情報と、該個人情報管理システムの個人情報とを結び付け、結び付けた連携情報は、該個人情報の利用条件情報と、該サービスシステムのサービスシステム情報から個人情報管理システムが許可した内容とによる利用制御に基づいた提供がなされる情報連携機能を有する個人情報統合管理システムにおいて、

前記情報連携機能は、

ＩＣカードに格納された個人情報を、ユーザＩＤを含む形で個人情報管理システムの個人情報データベースに格納する第一の事前処理ステップと、

サービスシステムにおいて顧客ＩＤと電子証明書とを作成し、サービスシステムＩＤと顧客ＩＤと証明書とをＩＣカードに格納し、サービスシステムＩＤと顧客ＩＤとを個人情報管理システムに格納する第二の事前処理ステップと、

ＩＣカードからサービスシステムに証明書を送信するサービス利用ステップと、

サービスシステムから個人情報管理システムに顧客情報とサービスシステムＩＤと顧客ＩＤとを送信する第一の連携処理ステップと、

個人情報管理システムにおいてサービスシステムＩＤと顧客ＩＤとを用いて個人情報データベースからユーザＩＤを特定する第二の連携処理ステップと、

個人情報管理システムにおいてユーザＩＤを用いて個人情報データベースから該ユーザＩＤに対応する個人情報を検索し、顧客情報と検索から得られた個人情報とを連携付ける第三の連携処理ステップとを含む処理によって実現されることを特徴とする個人情報統合管理システム。

【請求項２】　少なくともユーザの個人情報を格納したＩＣカードと、ＩＣカードとの間でデータを送受信するためのＩＣカードリーダライタを有するＩＣカードサービス端末と、ＩＣカードにＩＣカード用アプリケーションプログラムを提供するとともにＩＣカードサービス端末に端末用アプリケーションプログラムを提供し、各アプリケーションプログラムが起動したＩＣカード及びＩＣカードサービス端末を通じてユーザにサービスを提供する複数のＩＣカードサービスシステムであってそのうちの少なくとも１つはＩＣカードに格納されたユーザの個人情報を利用してユーザにサービスを提供する複数のＩＣカードサービスシステムと、ＩＣカードに格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システムと、ＩＣカードサービス端末と複数のＩＣカードサービスシステムと個人情報管理システムとを接続するネットワークとからなり、前記個人情報管理システムは、前記サービスシステムの要求に基づき、該サービスシステムの顧客情報と、該個人情報管理システムの個人情報とを結び付け、結び付けた連携情報は、該個人情報の利用条件情報と、該サービスシステムのサービスシステム情報から個人情報管理システムが許可した内容とによる利用制御に基づいた提供がなされる情報連携機能を有する個人情報統合管理システムのプログラムであって、

該プログラムはコンピュータ上に、

ＩＣカードに格納された個人情報を、ユーザＩＤを含む形で個人情報管理システムの個人情報データベースに格納する第一の事前処理ステップと、

サービスシステムにおいて顧客ＩＤと電子証明書とを作成し、サービスシステムＩＤと顧客ＩＤと証明書とをＩＣカードに格納し、サービスシステムＩＤと顧客ＩＤとを個人情報管理システムに格納する第二の事前処理ステップと、

ＩＣカードからサービスシステムに証明書を送信するサービス利用ステップと、

サービスシステムから個人情報管理システムに顧客情報とサービスシステムＩＤと顧客ＩＤとを送信する第一の連携処理ステップと、

個人情報管理システムにおいてサービスシステムＩＤと顧客ＩＤとを用いて個人情報データベースからユーザＩＤを特定する第二の連携処理ステップと、

個人情報管理システムにおいてユーザＩＤを用いて個人情報データベースから該ユーザＩＤに対応する個人情報を検索し、顧客情報と検索から得られた個人情報とを連携付ける第三の連携処理ステップとを含む処理によって前記情報連携機能を実現することを特徴とする個人情報統合管理システムのプログラム。

【請求項３】　請求項２に記載のプログラムを記録したことを特徴とするコンピュータ読み取り可能な媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数のＩＣカードサービスシステムで使用されるユーザの個人情報を、ユ

ーザ自身が主体的に管理し、かつＩＣカードサービスシステムに必要な個人情報の使用をユーザが設定した利用条件に基づいて制御する、個人情報統合管理システムを実現するための技術に関する。

【０００２】

【従来の技術】従来、サービスの提供者が、サービス利用履歴や趣味・嗜好等のユーザの個人情報を管理し、これをユーザに対するマーケティングに活用するケースが数多く見受けられていた。

【０００３】近年は、ＩＣカードを用いたＩＣカードサービスシステムを構築して、ユーザ情報の管理を行うシステムが増加している。これは、耐タンパ性に優れたＩＣカードの安全性を活用しようというもので、課金・決裁・資産管理サービスのような金銭の出納に関わるサービスや、電子行政・医療情報システムなど、繊細な情報やプライバシーに関わる情報を扱うサービスに対し、暗号・認証技術を用いた堅牢なユーザ認証を実現するために導入されたものである。

【０００４】ＩＣカードは、従来の磁気カードと比べ高コストであることから、複数のＩＣカードサービスシステムを１枚のカードで共用できるような高機能性が求められていたが、最近のＩＣチップの演算能力と記憶容量の向上に伴い、１枚のＩＣカードに複数のアプリケーション処理プログラムを搭載することができるようになった。これに併せ、ＩＣカードに搭載するアプリケーションについても、共通の開発環境と実行環境を提供するプラットフォームが開発されている（例えば、ＮＴＴ技術ジャーナル、２０００年１０月号、ｐ．１５－１８、ｐ５６－５９参照）。

【０００５】ＩＣカードサービスシステム開発の現状を見ると、ＩＣカード媒体の特徴である携行性と安全性を活かしたシステム構築がなされてはいるものの、ＩＣチップの演算処理能力を応用した高機能性の十分な活用には至っていないようである。

【０００６】具体的には、これまでのＩＣカードサービスシステムでは、ＩＣカードからＩＣカードサービスシステムにデータベース処理言語であるＳＱＬコマンドを送信することで、ＩＣカードサービスシステムの個人情報データベースに対する処理を実行する等、ＩＣカードに単なる情報蓄積媒体以上の機能を発揮させていた。

【０００７】しかし、ＩＣカード上での処理は、ＩＣカードに蓄積されていた該ＩＣカードサービスシステム向けに用意された処理プログラムとパラメータが選択され起動されるというものであり、高機能ＩＣカードサービスシステムの使い道としては比較的容易な処理内容に過ぎなかった。

【０００８】一方、ＩＣカードサービスシステムで使用される個人情報については、上述したように、従来からマーケティングに役立つ情報として認められていたが、近年の通信ネットワークの普及に伴う電子サービスの中て、電子化された個人情報を用いることで容易に実現されるようになったマス・カスタマイゼーションが、マーケティング戦略面のみならず、効率面でも有効であることが判明すると、特に電子化された個人情報の価値はますます増大してきた。事実、通信ネットワーク上でのサービス提供企業が売却される際に、該企業の有する個人情報が重要な資産価値として認められもしている。

【０００９】しかしながら、個人情報が電子化され通信ネットワーク上で利用されることには、ユーザとして安全面での懸念がある。セキュリティ、プライバシーの問題がそれである。個人情報保護に関する法律制定の動きもあるが、ユーザも自己防衛を考えるようになり、また、サービス提供者としても信用問題につながるため、相当の力を入れるようになってきつつある。

【００１０】通信ネットワークにおける個人情報流通を技術面から支えるため、暗号・認証やデータ利用制御技術が開発され、後者においては、ユーザがユーザ自身の個人情報に利用条件を課す方法が考案されている（例えば、寺西裕一　他「利用規約に基づくマルチメディアコンテンツ流通システムの設計」情処研報９９－ＤＰＳ－９５、Ｖｏｌ．９９、Ｎｏ．９４、１９９９、ｐｐ３１－３６参照）。これは、個人情報の管理に対しユーザが主導権を持つことにつながり、また、個人情報が通信ネットワーク上を流通する世界を想定したものでもある。

【００１１】

【発明が解決しようとする課題】このような状況の下、多数のＩＣカードサービスシステム導入の動きがあるが、現状のままでＩＣカードサービスシステムの構築が進められると、ユーザの個人情報が複数のＩＣカードサービスシステムで独立に存在し、各ＩＣカードサービスシステムで管理されることになる。すると、ユーザの個人情報は各ＩＣカードサービスシステムで管理され、ＩＣカードサービスシステムの数だけ存在することになるので、ユーザは利用したいシステムの数だけＩＣカードを携帯する必要が生じ、ユーザ自身の個人情報であるにも拘わらず、ユーザ自身で管理することができず、ユーザの個人情報に何らかの変更が生じた場合、複数のシステムに対してそれぞれ個人情報更新処理を行わなければならなくなる。また、ユーザはユーザ自身の個人情報がどこでどのように使用されているか把握できず、個人情報がユーザの意図に沿わない使われ方をされる可能性がある。また、派生的課題として、ＩＣカードサービスシステム間で個人情報を流通する際に、ユーザが予想していないシステム間の情報連携により、個人のプライバシーに関わる情報が生じる危険がある。

【００１２】そこで、本発明では、ＩＣカードサービスシステム毎に管理されているユーザの個人情報を、ユーザ自身が管理できるようにし、各ＩＣカードサービスシステムが必要とする個人情報をユーザが許可した条件の下でのみ利用可能とし、ＩＣカードサービスシステムに

提供した個人情報の使われ方を制御でき、特に、複数のＩＣカードサービスシステムの情報連携によってユーザの意図しない個人情報が作り出されることがない個人情報統合管理システムを提供することを目的とする。

【００１３】

【課題を解決するための手段】上記の課題を解決するために、本発明では、ＩＣカードの多機能性を従来以上に発揮させ、１枚のＩＣカードに複数のサービス処理機能を持たせてワンカード化を図り、また、暗号・認証技術と利用制御技術を利用して、個人情報の安全な流通の仕組みを設ける。そして、ＩＣカードと複数のＩＣカードサービスシステムが相互に情報連携しての処理が可能となるＩＣカードサービス環境を構築する。

【００１４】具体的には、ＩＣカード上に、個人情報と該個人情報の利用条件情報とを蓄積し、更に、複数のＩＣカードサービスシステムのＩＣカードにおける処理プログラム（カード用サービスＡＰ）及びこれに用いる情報（ＡＰ個人情報）を、複数サービス分だけ搭載する。この時、ＩＣカードサービスシステムの１つとして、ユーザの個人情報を管理するサービスを行う個人情報管理システムを用意し、該システムのＩＣカードにおける処理プログラム（カード用管理ＡＰ）をＩＣカードに搭載しておく。

【００１５】個人情報管理システムは、複数のユーザの個人情報及び各個人情報に課した利用条件情報及び通常の各ＩＣカードサービスシステム（以下、サービスシステムと略す）のＡＰ個人情報を各ユーザが主体となって管理する機能と、各ユーザの個人情報を各ユーザの利用条件情報に基づいて制御する機能を、個人情報管理システムのサービスとして提供する。また、個人情報管理システムは、サービスシステム情報を管理する機能を有する。そして、あるサービスシステムに対する個人情報を用いた処理においては、該サービスシステムに対応するサービスシステム情報と個人ＡＰ情報を参照することで、個人情報の利用制御や、情報連携サービスや、カード用サービスＡＰの処理制御を行う。

【００１６】一方、システム間での情報連携が個人のプライバシーを侵害するのを防ぐために、サービスシステムの顧客情報と、管理システムの個人情報を匿名のまま関連付ける仕組みを設ける。

【００１７】個人情報管理システムにおけるユーザ認証や、サービスシステムにおける顧客認証には、公開鍵暗号方式を用いたチャレンジ＆レスポンスによる認証を用いる。

【００１８】ＩＣカードには、サービスシステムの顧客認証に用いる鍵ペアを用意しておき、サービスシステムに公開鍵を送信する。

【００１９】サービスシステムでは、ユーザ用に作成した顧客ＩＤと受信した公開鍵に対しサービスシステム固有の暗号鍵により署名を行った電子証明書（以下、証明書）を作成し、ＩＣカードに送信する。

【００２０】個人情報管理システムでは、サービスシステムＩＤと顧客ＩＤとからユーザＩＤを検索できるようなデータベースを構築する。

【００２１】

【作用】本発明の個人情報統合管理システムは、個人情報管理サービスを提供する個人情報管理システムと、各種サービスを提供する複数のサービスシステムと、カードリーダライタが付属したＩＣカードサービス端末と、そして、各ユーザの個人情報等を蓄積したＩＣカードにより構成される。ＩＣカード上には、個人情報管理システムで管理する個人情報と該個人情報の利用条件情報とを蓄積し、更に、複数のサービスシステムのカード用サービスＡＰ及びＡＰ個人情報を搭載する。

【００２２】個人情報統合管理システムでは、ＩＣカードサービスシステムの１つとして個人情報管理システムを用意し、ユーザの個人情報を管理するサービスを行う。個人情報管理サービスを利用するには、ＩＣカードサービス端末で、カード用個人情報管理ＡＰ（カード用管理ＡＰ）をＩＣカードに予めダウンロードする。そして、ユーザはＩＣカードサービス端末（カード端末）で個人情報管理サービスのクライアントプログラム（端末用管理ＡＰ）を起動する。

【００２３】個人情報管理システムは、複数のユーザの個人情報及び各個人情報に課した利用条件情報及び各サービスシステムの個人ＡＰ情報を各ユーザが主体となって管理する機能と、各ユーザの個人情報を各ユーザの利用条件情報に基づいて制御する機能を、個人情報管理システムのサービス（管理サービス）として提供する。

【００２４】ユーザが各サービスシステムのサービスを利用するには、カード端末で、利用する各サービスシステムのカード用サービスＡＰを予めＩＣカードにダウンロードする。そして、ユーザはＩＣカードサービス端末（カード端末）で利用したいサービスシステムのクライアントプログラム（端末用サービスＡＰ）を起動する。端末用サービスＡＰは、カード用管理ＡＰが管理する個人情報及び利用条件情報と、カード用サービスＡＰが管理する個人ＡＰ情報を利用して、各サービスシステムが提供する様々な処理を行う。

【００２５】個人情報管理システムの管理サービスは、サービスシステムの個人情報要求に対し、ユーザが設定した個人情報と利用条件情報とを用い、ユーザが許可した範囲で個人情報を提供する。ＩＣカードがシステムに接続されていない場合も、管理サービスは利用条件付き個人情報を提供できる。

【００２６】個人情報管理システムとサービスシステムとの情報連携については、サービスシステムから個人情報管理システムに情報連携処理要求があると、個人情報管理システムはサービスシステムＩＤと顧客ＩＤとからデータベースを検索し、ユーザＩＤを特定し、該ユーザ

ＩＤの個人情報と関連付ける。この関連付け処理では、ユーザＩＤをシステム処理の工程内でのみ使用しているので、結果を抽出する前に利用条件に基づく利用制御を行うことで、プライバシーを侵害するような情報連携を避けることができる。

【００２７】

【発明の実施の形態】本発明の個人情報統合管理システムの実施の形態の一構成例について、図１を用いて説明する。

【００２８】図１において、１０はＩＣカード、２０はＩＣカードサービス端末（以下、カード端末と略す）、３０は複数の通常のＩＣカードサービスシステム（以下、サービスシステムと略す）、４０は個人情報管理システム、５０はネットワークである。

【００２９】本発明の個人情報統合管理システムでは、カード端末２０と、複数のサービスシステム３０と、個人情報管理システム４０とがネットワーク５０を介して接続されている。これらに加え、各ユーザのＩＣカード１０が、単体では機能しないが、カード端末２０のＩＣカードリーダライタ（ＩＣカードＲＷ）２１に挿入されることでシステムの一部として動作する。

【００３０】更に、システムには、ユーザが初めてＩＣカードサービス環境である個人情報統合管理システムにアクセスしようとする際に、該ユーザに初期情報を記録したＩＣカードを発行する個人情報登録システムが接続されていても良い。本発明ではこの個人情報登録システムを必須の構成要素とはしないが、個人情報統合管理システムの中で絶対の信頼機関として個人情報登録システムを使用する構成も可能である。

【００３１】いずれにせよ、本システムでは、それぞれが通信を行うために信頼関係を保たなければならないので、接続の際に相互認証を行う。具体的には、ＩＣカード１０はカード端末２０に挿入する際に、また、カード端末２０とサービスシステム３０と個人情報管理システム４０とはネットワーク５０で接続する際に相互認証を行う。

【００３２】相互認証には、個人情報登録システムなどにおいて発行された証明書を用い、公開鍵暗号方式を用いたチャレンジ＆レスポンスにより互いに認証することで相互認証を行う。

【００３３】証明書は、申請者が作成した鍵ペアの公開鍵及び登録システムが発行したＩＤに対し、登録システム固有の暗号鍵により署名を行うことにより作成する。

【００３４】これら個人情報統合管理システムを構成する各構成要素が格納・管理している情報を図２に示す。項目に記した具体的なプロパティは、情報のカテゴリを分かり易く示すための例である。また、ＩＣカードは記憶容量に制限があるので、カード用管理アプリケーションプログラム（ＡＰ）で蓄積するデータはポインタとして機能する情報であっても良い。

【００３５】ＩＣカード１０にはユーザの個人情報が格納されている。個人情報には、ユーザを特定する又はユーザを特徴づけるための住所、氏名、年齢、性別、趣味、嗜好……といった情報等の基本情報と、各サービスシステムのアプリケーションを利用する際に必要なサービスシステム用個人情報と、個人情報管理システム及び各サービスシステムを介して利用してきたログ情報である個人履歴情報と、そして、これら基本情報・サービスシステム用個人情報・個人履歴情報の個々の項目についての利用条件を定めた利用条件情報とがある。

【００３６】サービスシステム３０には、サービスシステム情報と、顧客情報とが格納されている。サービスシステム情報は、該サービスシステムが主体となって管理する、サービスシステムを特定・識別する又はサービスシステムの特徴を示す情報である。顧客情報は、該サービスシステムが主体となって管理する、サービスシステム利用ユーザ毎に取得した情報である。

【００３７】個人情報管理システム４０では、ユーザが主体となって管理している、ＩＣカードに格納する個人情報の全て又は個人情報に課せられた利用条件情報が個人情報管理システムに許す範囲の個人情報を格納している。加えて、サービスシステムが主体となって管理しているサービスシステム情報を、各サービスシステムの分だけ管理している。

【００３８】個人情報統合管理システムを利用しようとするユーザは、ユーザ自身の個人情報を管理するために、個人情報管理システム４０の個人情報管理サービス（管理サービス）を使用する。ＩＣカード情報を可視化し、情報を操作するソフトウェアがあれば管理はできるが、ＩＣカード情報をオンラインで扱うためには、個人情報管理システムが必要になる。

【００３９】個人情報管理サービスの概要を図３及び図４を用いて説明する。

【００４０】図３は個人情報管理システムの概要を示すもので、図中、４１は個人情報データベース、４２はサービスシステムデータベース、４３は個人情報管理モジュール、４４はサービスシステム管理モジュール、４５は利用制御モジュールである。また、図４は個人情報管理サービスの処理の流れを示す。

【００４１】初めて個人情報管理システム４０にアクセスするユーザは、予めカード端末２０でＩＣカード１０にカード用個人情報管理ＡＰ（以下、カード用管理ＡＰと略す）１１をダウンロードする。そして、管理サービスを利用する場合、ユーザはカード端末２０で端末用個人情報管理ＡＰ（以下、端末用管理ＡＰと略す）２２を起動し、カード端末２０のＩＣカードＲＷ２１に挿入したＩＣカード１０上のカード用管理ＡＰ１１を用いて、個人情報及び各個人情報に対する利用条件の設定など、個人情報管理の操作を行う。

【００４２】ユーザは、管理サービスを利用して設定し

た個人情報及び利用条件情報の原本を、ＩＣカード１０上のカード用管理ＡＰ１１に保存する。個人情報管理システム４０の個人情報管理モジュール４３では、カード用管理ＡＰ１１の個人情報と利用条件情報を、管理システム４０に対し定めた利用条件の範囲で個人情報管理システム４０の個人情報ＤＢ４１に保存する。個人情報管理システム４０に対して定める個人情報の利用条件としては、個人情報の全てを取り扱うことができるように特権システムとして定めることが望ましいが、必要ならば適当な利用条件を定めることで利用制御させることも可能である。

【００４３】尚、個人情報管理システム４０中、サービスシステムＤＢ４２、サービスシステム管理モジュール４４及び利用制御モジュール４５については、図７，８を用いて後ほど説明することとし、管理サービスの処理の流れを説明する。

【００４４】カード端末２０で端末用管理ＡＰ２２を起動しておき、そこにＩＣカード１０が挿入されるとＩＣカード１０上のカード用管理ＡＰ１１が起動され、管理サービスが可能になる。カード用管理ＡＰ１１は、本管理サービスのサービス認証を行い、該サービスに対する利用条件を判断の上、開示制御を加えた個人情報の読み出しを行う。

【００４５】一方、個人情報管理システム４０の個人情報管理モジュール４３は、ＩＣカード利用者のユーザ認証を行い、システム上の個人情報ＤＢ４１から利用条件を判断しながら個人情報の読み出しを行う。これらの個人情報は端末用管理ＡＰ２２に送信され、具体的なユーザの管理操作を受け付ける管理サービスが提供される。

【００４６】ユーザがカード端末２０で個人情報操作の管理サービス処理を行うと、処理内容に応じ、ＩＣカード１０または個人情報管理システム４０に処理内容が送信、処理される。処理が終わればカード端末２０に処理完了の通知が返り、ＩＣカード１０上のカード用管理ＡＰ１１が終了し、カード端末２０での操作に従い、ＩＣカード１０が排出される。

【００４７】次に、サービスシステムによる提供サービスの概要を図５及び図６を用いて説明する。

【００４８】図５はサービスシステムの概要を示すもので、図中、３１はサービスシステム顧客データベース、３２はサービス処理モジュールである。また、図６はサービスシステムにおける提供サービスの処理の流れを示す。

【００４９】初めてサービスシステム３０にアクセスするユーザは、カード用管理ＡＰ１１に加え、カード用サービスＡＰ１２をＩＣカード１０に搭載しておく必要があり、予めカード端末２０で該サービスのカード用サービスＡＰ１２をＩＣカード１０にダウンロードしておく。

【００５０】サービスシステム３０のサービスを受けるには、カード端末２０で端末用サービスＡＰ２３を起動する。この時、既にＩＣカード１０に搭載されているカード用管理ＡＰ１１で保存している個人情報が、サービスに対し定められた利用条件情報の下で利用可能になる。端末用サービスＡＰ２３は、必要に応じてＩＣカード１０上のカード用サービスＡＰ１２及びカード用管理ＡＰ１１と連携して、必要な個人情報を該サービスに課せられた利用条件情報に基づき利用しつつ、該サービスのサービス処理を遂行する。

【００５１】サービスシステム３０では、サービス処理モジュール３２を介し、カード用管理ＡＰ１１によって利用制御された個人情報を用いてサービス処理が行われ、サービスシステム３０が自身で収集したユーザ情報を顧客情報として収集する。

【００５２】サービスシステム３０の処理の流れとしては、まず、カード端末２０で端末用サービスＡＰ２３を起動しておき、そこにＩＣカード１０を挿入する。サービスシステム３０では、ＩＣカード利用者の顧客認証を行い、サービスシステム３０に格納されているサービスシステム情報を読み出す。ＩＣカード１０では、カード用サービスＡＰ１２の前にカード用管理ＡＰ１１が起動される。カード用管理ＡＰ１１はサービスシステム情報を参照し、利用しようとしているサービスシステム３０の認証を行う。そして、該サービスに対する利用条件を判断の上、開示制御を加えた個人情報の読み出しを行う。

【００５３】ＩＣカード１０上で動作するＡＰの制約から、ＡＰの複数起動が可能な場合と不可能な場合とがある。図６の例では、カード用管理ＡＰ１１とカード用サービスＡＰ１２の双方のＡＰが同時に起動しないと仮定して、カード用管理ＡＰ１１を終了させた後、カード用サービスＡＰ１２を起動している。

【００５４】カード用サービスＡＰ１２の起動を受けて、端末用サービスＡＰ１１はＩＣカード１０からサービスに用いる情報の読み出しを行い、また、サービスシステム３０からは顧客ＤＢ３１から顧客情報の読み出しを行う。これらの情報は端末用サービスＡＰ２３に送信され、具体的なユーザの操作を受け付けるサービス提供が開始される。ユーザがカード端末２０でサービス操作を行うと、処理内容に応じ、ＩＣカード１０またはサービスシステム３０に処理内容が送信、処理される。

【００５５】ＩＣカード１０とサービスシステム３０での各々の処理の結果、必要に応じてＩＣカード１０または顧客ＤＢ３１に処理情報の書き込みが行われる。処理が終わればカード端末２０に処理完了の通知が返り、ＩＣカード１０上のカード用サービスＡＰ１２が終了し、カード端末２０での操作に従い、ＩＣカード１０が排出される。

【００５６】次に、個人情報管理システムの個人情報ＤＢとサービスシステムの顧客情報ＤＢとを連携させるサ

ービスについて図７及び図８を用いて説明する。図７は個人情報管理システム及びサービスシステムの概要を示す。また、図８は連携サービスの処理の流れを示す。

【００５７】サービスシステム３０は、ＩＣカード１０との接続を必要としない処理が目的で個人情報を扱おうとする場合や、統計処理などユーザ一般に関する情報を用いた処理を行う場合等に、個人情報管理システム４０の管理サービスを利用する。サービスシステム３０の顧客情報と個人情報管理システム４０の個人情報を連携させるには、各データベースにユーザを特定するためのキーを設定しておく。この方法の詳細は図９を用いて別途説明する。

【００５８】さて、個人情報管理システム４０の個人情報管理サービスを利用するサービスシステム３０は、個人情報管理システム４０のサービスシステム管理モジュール４４を介し、サービスシステムＤＢ４２にサービスシステム情報を登録しておく必要がある。サービスシステム情報の具体的な項目としては、サービスシステム毎に振られたサービスシステムＩＤ、サービスシステムの正当性を認証するための情報、サービスシステムの提供するサービスのカテゴリや特徴的キーワード等が挙げられる。

【００５９】個人情報管理システム４０は、サービスシステム３０の要求に対しサービスシステム管理モジュール４４でサービスシステムとしての認証等の処理を行い、利用制御モジュール４５で該サービスシステム３０の利用条件を判断し、許された範囲内で個人情報ＤＢ４１から個人情報を抽出し、該個人情報をサービスシステム３０に送信する。あるいは定められた利用条件によっては、逆に個人情報管理システム４０で該情報を用いた処理を行い、許可された結果のみをサービスシステム３０に送信する。

【００６０】個人情報管理システムとサービスシステムとの情報連携処理の流れとしては、まず、サービスシステム３０から個人情報管理システム４０へ、管理サービス利用のためのアクセス要求が送信される。管理システム４０はアクセス要求したサービスシステム３０の認証を行い、サービスシステムＤＢ４２からサービスシステム情報の読み出しを行う。

【００６１】サービスシステム３０は、更に、サービスシステム３０で得られている顧客情報と個人情報に基づき、管理サービスの個人情報利用要求を送信する。すると管理システム４０は、サービスシステム３０の顧客ＩＤに対応する個人情報との関連付けを行う。関連付けの方法は、先にも述べたように後述する。管理システム４０は、関連付けられた個人情報を個人情報ＤＢ４１から読み出し、該個人情報の利用条件を解析し、利用条件付き個人情報を生成する。サービスシステム３０は、自ら所有する顧客情報に利用条件を設定して、これを管理システム４０に送付する。

【００６２】この時点で個人情報管理システム４０にユーザに関する各種情報が取り揃えられたことになるが、個人情報管理システム４０では、利用制御モジュール４５において、個人情報と顧客情報を連携させ、連携情報に対しどのような利用条件情報を付与すれば良いかの解析を行う。そして、その判断に基づき、利用条件付きの連携情報が生成され、管理サービスの処理結果としてサービスシステム３０に利用条件付き連携情報を引き渡す。

【００６３】以上が一連の処理の流れであるが、利用条件に依っては、最後の工程で連携情報がサービスシステム３０に引き渡されず、個人情報管理システム４０上でのみ取り扱い可能な状態になることもある。このような時、もしもサービスシステム３０に連携情報入手の許可は無くても、連携情報を使った別の処理が許可されていれば、個人情報管理システム４０の利用制御モシュール４５において処理が行われ、サービスシステム３０に処理結果を返送することになる。

【００６４】次に、ＩＣカード１０から個人情報管理システム４０に送信され格納されている個人情報とサービスシステム３０に格納されている顧客情報との連携サービスの実現例を図９を用いて説明する。ここでは、不必要な個人情報の公開を防ぐため、匿名性を維持しつつ顧客情報に対応する連携先個人情報を判断する方法を例示する。

【００６５】個人情報管理システム４０には、ＩＣカード１０の個人情報が、ユーザが設定した利用条件と共に格納されている（ステップ１－１）。次に、ＩＣカード１０またはカード端末２０において鍵ペアを作成し、格納する（ステップ１－２）。

【００６６】サービスを利用する際は、まず、公開鍵をサービスシステム３０に送信する（ステップ２－１）。公開鍵を受信すると、サービスシステム３０は顧客ＩＤを発行し、顧客ＩＤと公開鍵にサービスシステム固有の暗号鍵で署名を行うことにより証明書を作成する（ステップ２－２）。そして、ＩＣカード１０にサービスシステムＩＤと顧客ＩＤと証明書とを格納し（ステップ２－３）、また、ユーザは個人情報管理システム４０の個人情報ＤＢ４１にサービスシステムＩＤと顧客ＩＤとを格納しておく（ステップ２－４）。

【００６７】ユーザがサービスシステム３０のサービスを受ける際には、証明書をサービスシステム３０に送信し、相互認証を行う。

【００６８】サービスシステム３０は、ユーザがサービスを利用する際にユーザから取得した顧客情報を、個人情報管理システム４０の個人情報と連携させるために、まず、サービスシステム３０から個人情報管理システム４０にサービスシステムＩＤと顧客ＩＤとを送信する（ステップ３－１）。

【００６９】個人情報管理システム４０では、サービス

システムＩＤと顧客ＩＤとから個人情報ＤＢ４１を検索し、ユーザＩＤを特定する（ステップ３－２）。得られたユーザＩＤを基に個人情報ＤＢ４１を検索し、顧客情報と連携させるべき個人情報を得る（ステップ３－３）。

【００７０】個人情報管理システム４０の利用制御モジュール４５は、サービスシステム３０に許可された利用条件を判断し、サービスシステム３０に提供を許された情報については利用制御を課したまま、個人情報管理システム４０からサービスシステム３０に送信する。サービスシステム３０への該個人情報の提供は許されていないが、顧客情報と個人情報とを用いて行う何らかの処理の結果を知ることが許可されている場合、サービスシステム３０から個人情報管理システム４０へ該顧客情報を送信し、個人情報と連携させて実行した処理結果をサービスシステム３０に返送する。

【００７１】サービスシステム３０が、個人情報の提供も個人情報を用いた処理の実行も許されていない場合、サービスシステム３０から個人情報管理システム４０への情報連携要求は不成功に終わる。

【００７２】情報連携を用いた具体的な実施サービス例として、また、本発明の個人情報統合管理システムの発展的サービス例として、サービスシステムが顧客情報と個人情報との連携情報を統計情報として顧客動向調査に利用し、抽出した個人に対し広告を配送するサービスについて述べる。

【００７３】あるサービスシステム（例えば、ＳＳ－Ａとする）の顧客情報ＤＢにサービス履歴情報を蓄積しておく。仮に、ＳＳ－Ａが、ＳＳ－Ａの提供するサービス甲を受けた顧客に特徴的な傾向を発見したとする。ＳＳ－Ａは個人情報管理システム４０と連携して、前記の特徴的な傾向を見せた顧客の顧客ＩＤと、情報から関連付けられたユーザの個人情報を統計的に提供してもらう。

【００７４】この時のユーザの利用条件では、例えば「母数１００以上の統計処理への利用を許可」等の設定がなされている必要があり、そのような提供を許可していないユーザの個人情報は、統計情報としても提供されない。ＳＳ－Ａは、情報連携で得られた統計情報の分析の結果、例えば「サービス甲を受け、引き続きサービス乙を利用する顧客は２０代女性に多数見られる」等のマーケティング情報を得ることができる。

【００７５】上記マーケティング情報を得たＳＳ－Ａは、サービス甲の利用ユーザの中でまだサービス乙を利用していない顧客に何らかの働きかけを行う、または広く一般ユーザに対して働きかけを行うと考えられる。その働きかけの手段として広告配送による方法がある。しかし、広告配送先である住所情報は、個人情報の１項目であり、ＳＳ－Ａに公開されるとは限らない。そこで、信用できる機関が広告配送サービスを行う仲介することが考えられる。

【００７６】図９における説明では、個人情報管理システムを信用できる機関として、個人情報管理システムで情報連携を行う例を記した。しかし、広告配送専用のサービスシステムＢ（例えば、ＳＳ－Ｂ）が信用できるか、またはＳＳ－Ｂが利用条件を課せられた上でサービスを提供するならば、情報連携をＳＳ－Ｂで行う方法も採ることができる。実現には、暗号・認証技術と、カプセル化等を用いた利用制御技術を用いた方法が考えられる。

【００７７】ＳＳ－Ｂが該サービスを提供する場合、ＳＳ－Ａは広告情報をカプセル化し、広告情報の内容だけでなくＳＳ－Ａが発信者であることも掌握できないような利用条件と共にＳＳ－Ｂに送り、ＳＳ－Ｂは対応するユーザの個人情報から住所（電子メール広告の場合はメールアドレス）を調べ、関連付けることだけが可能な利用条件を課せられているが、該ユーザのもとに広告情報を配送することは実現できる。

【００７８】

【発明の効果】以上述べたように、本発明では、ユーザがサービスシステム毎に用意した鍵ペア及びサービスシステムが発行した顧客ＩＤを用いて匿名のまま顧客登録を行い、ユーザが顧客ＩＤ及び公開鍵を個人情報管理システムにのみ公開し、ユーザ個人情報として登録することで、個人情報管理システムを介することなく顧客認証を行うことができる。サービスシステムがユーザの身元確認を必要とする場合は、サービスシステムが個人情報管理システムに問い合わせることで匿名のまま身元証明を行うことができる。また、ユーザが匿名でサービスを受けるための識別情報をサービスシステム毎に個別に用意することで、複数のサービスシステムで格納されている個人情報を識別情報を用いて連携させ、ユーザが意図しない個人情報を作り出すという行為を制限することができる。

【図面の簡単な説明】

【図１】本発明の個人情報統合管理システムの実施の形態の一例を示す構成図

【図２】本システムの各構成要素に格納される個人情報の具体例を示す説明図

【図３】個人情報管理システムの概要を示す構成図

【図４】個人情報管理サービスの処理の流れ図

【図５】サービスシステムの概要を示す構成図

【図６】サービスシステムにおける提供サービスの処理の流れ図

【図７】個人情報管理システム及びサービスシステムの概要を示す構成図

【図８】個人情報管理システムとサービスシステムとの連携サービスの処理の流れ図

【図９】連携サービスの実現例を示す説明図

【符号の説明】

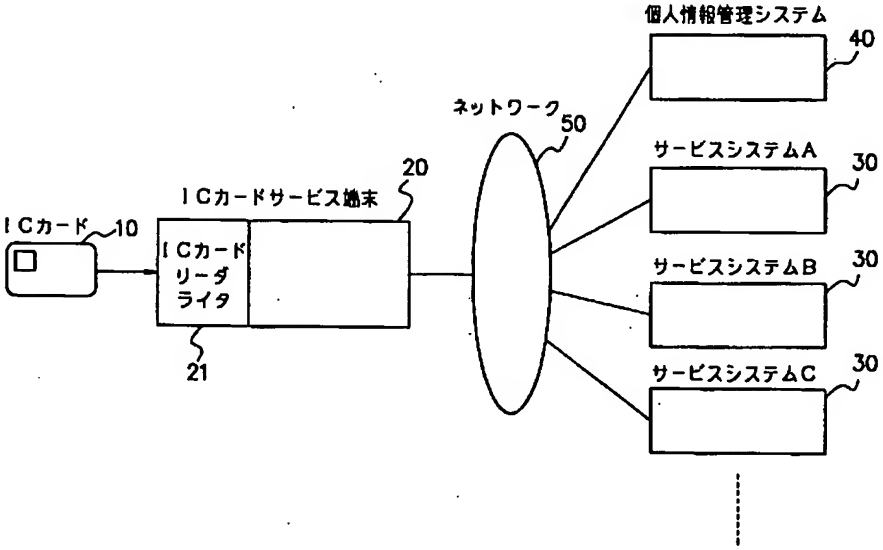
１０：ＩＣカード、１１：カード用管理ＡＰ、１２：カ

15

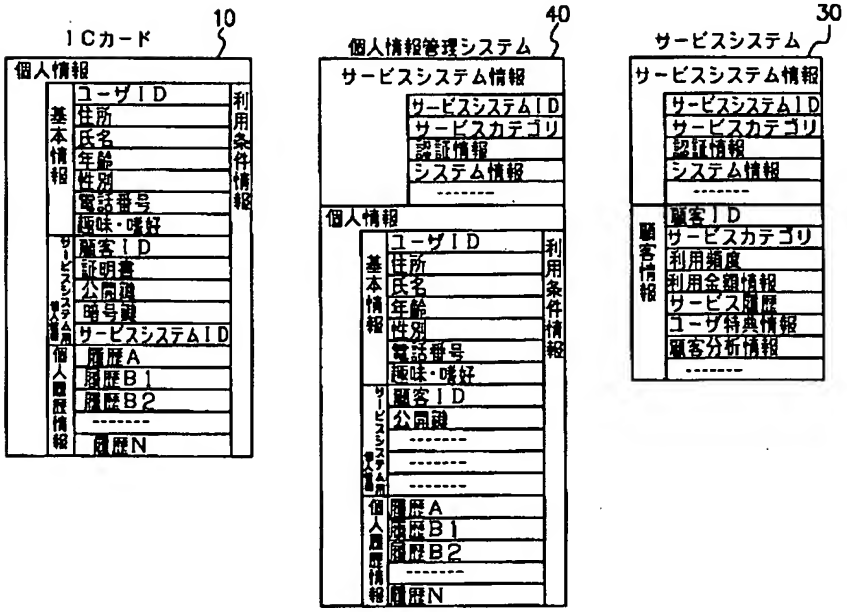
ード用サービスＡＰ、２０：ＩＣカードサービス端末、２１：ＩＣカードＲＷ、２２：端末用管理ＡＰ、２３：端末用サービスＡＰ、３０：サービスシステム、３１：サービスシステム顧客ＤＢ、３２：サービス処理モジュール、４０：個人情報管理システム、４１：個人情報ＤＢ、４２：サービスシステムＤＢ、４３：個人情報管理モジュール、４４：サービスシステム管理モジュール、４５：利用制御モジュール、５０：ネットワーク。

16

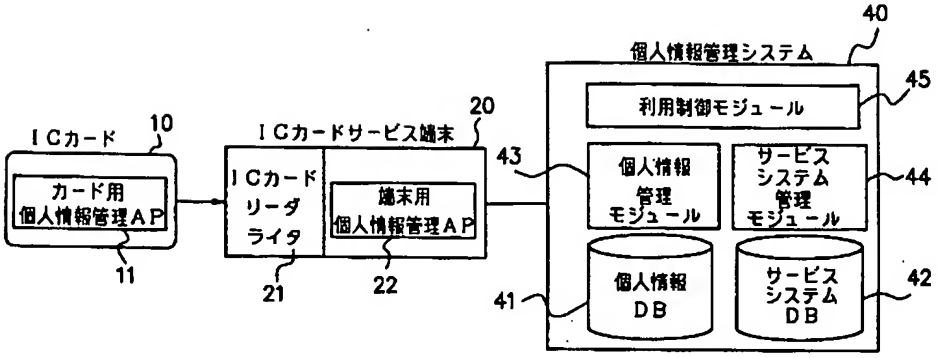
【図１】



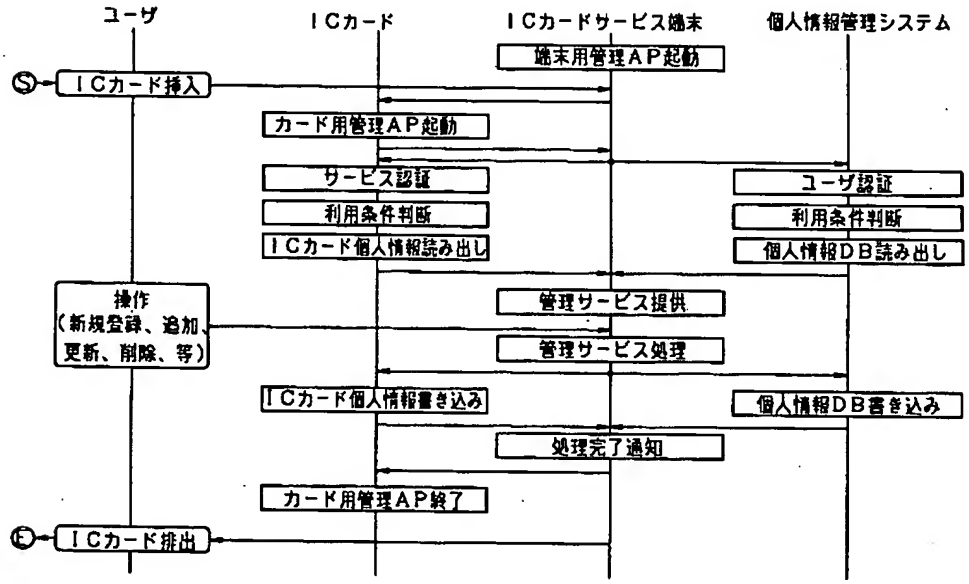
【図２】



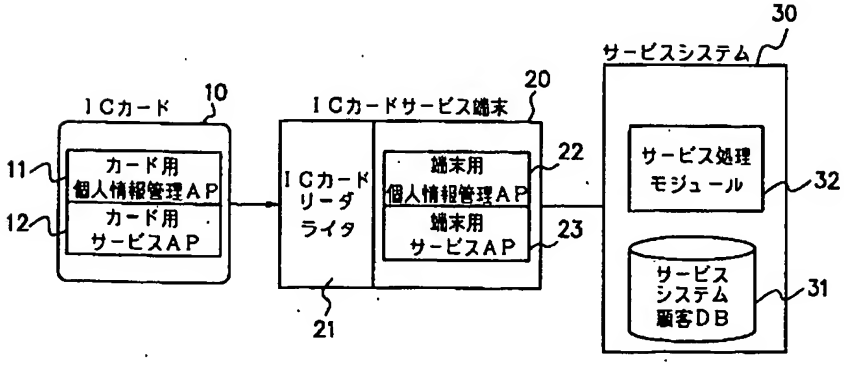
【図３】


40
個人情報管理システム
45
利用制御モジュール
ＩＣカード
10
ＩＣカードサービス端末
20
43
個人情報管理モジュール
サービスシステム管理モジュール
44
カード用個人情報管理ＡＰ
ＩＣカードリーダライタ
端末用個人情報管理ＡＰ
11
21
22
41
個人情報ＤＢ
サービスシステムＤＢ
42

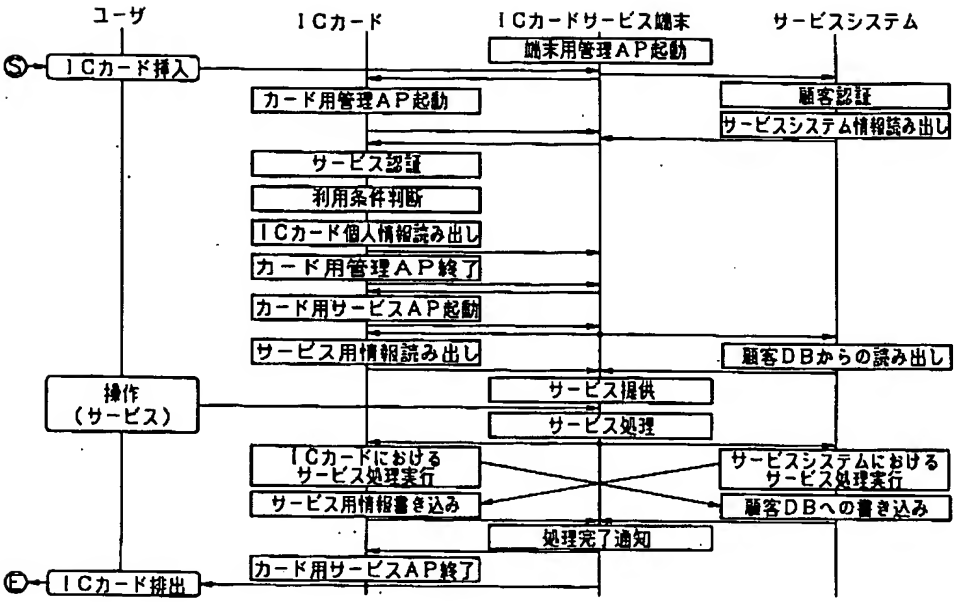
【図４】


ユーザ
ＩＣカード
ＩＣカードサービス端末
個人情報管理システム
端末用管理ＡＰ起動
ＩＣカード挿入
カード用管理ＡＰ起動
サービス認証
ユーザ認証
利用条件判断
利用条件判断
ＩＣカード個人情報読み出し
個人情報ＤＢ読み出し
操作（新規登録、追加、更新、削除、等）
管理サービス提供
管理サービス処理
ＩＣカード個人情報書き込み
個人情報ＤＢ書き込み
処理完了通知
カード用管理ＡＰ終了
ＩＣカード排出

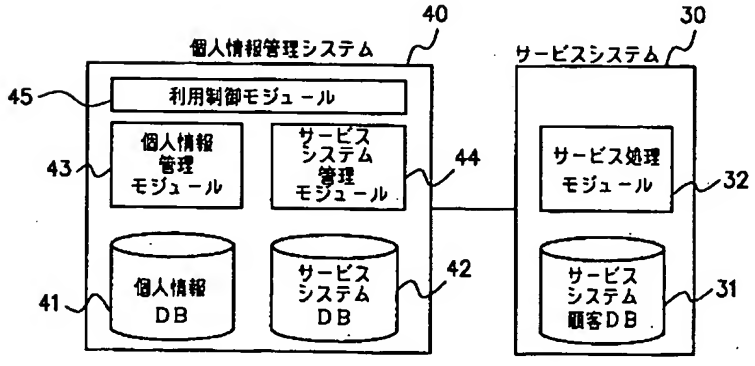
【図５】


30
サービスシステム
ＩＣカード
10
ＩＣカードサービス端末
20
11
カード用個人情報管理ＡＰ
12
カード用サービスＡＰ
ＩＣカードリーダライタ
端末用個人情報管理ＡＰ
22
端末用サービスＡＰ
23
サービス処理モジュール
32
サービスシステム顧客ＤＢ
31
21

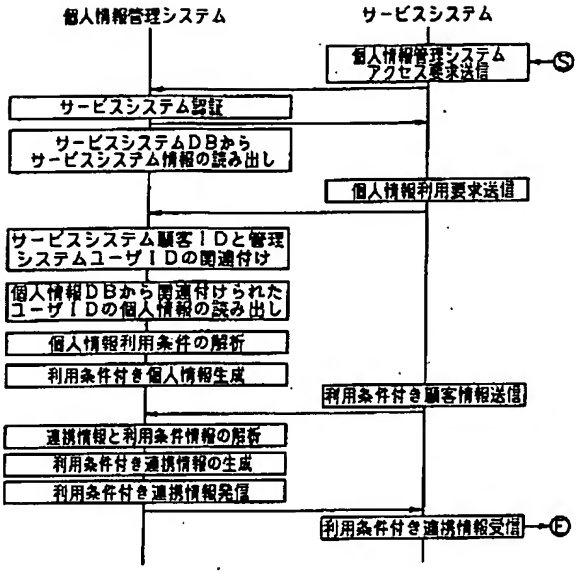
【図６】


ユーザ
ＩＣカード
ＩＣカードサービス端末
サービスシステム
Ｓ
ＩＣカード挿入
端末用管理ＡＰ起動
カード用管理ＡＰ起動
顧客認証
サービスシステム情報読み出し
サービス認証
利用条件判断
ＩＣカード個人情報読み出し
カード用管理ＡＰ終了
カード用サービスＡＰ起動
サービス用情報読み出し
顧客ＤＢからの読み出し
操作
（サービス）
サービス提供
サービス処理
ＩＣカードにおける
サービス処理実行
サービスシステムにおける
サービス処理実行
サービス用情報書き込み
顧客ＤＢへの書き込み
処理完了通知
カード用サービスＡＰ終了
Ｅ
ＩＣカード排出

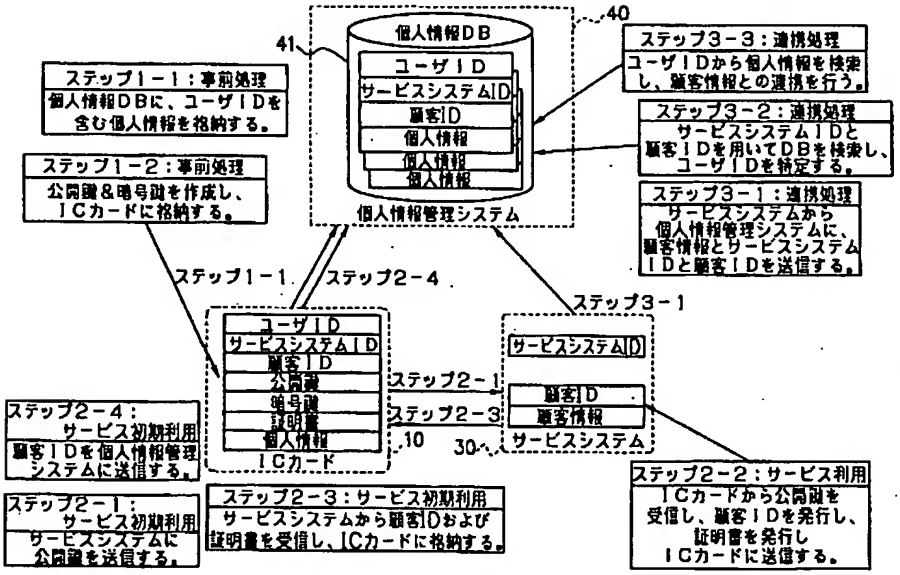
【図７】


40
30
個人情報管理システム
サービスシステム
45
利用制御モジュール
43
個人情報
管理
モジュール
サービス
システム
管理
モジュール
44
サービス処理
モジュール
32
41
個人情報
DB
サービス
システム
DB
42
サービス
システム
顧客DB
31

【図８】



【図９】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI			テーマコード (参考)
15/00	330	15/00	330	G	5B085
17/30	170	17/30	170	Z	
17/60	330	17/60	330		
	510		510		

(72)発明者　西田　玄
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　2C005 MA04 MB01 MB08 MB10 NA02
SA02 SA06 SA12 SA13 SA22
SA25 SA30 TA21
5B017 AA03 BA05 CA14
5B058 CA25 KA02 KA04 KA08 KA31
KA35 YA20
5B075 KK02 ND20 UU08
5B082 EA12 JA08
5B085 AA08 AE01 AE06 AE12 AE23
BA07 BG07